BROCKIT

PHIPA Compliance

An introduction to the Personal Health Information Protection Act

Part 1 of the 3 part Webinar series on PHIPA compliance.

Part 1: **Securing your clients health Data, Understanding PHIPA compliance** (March 18th 2025)

Part 2: **Managing PHIPA Breaches: Essential Steps for Healthcare Providers** (April 22nd 2025)

Part 3: **Preparing for the Worst: A PHIPA Breach Tabletop Exercise** (May 20th 2025)

What we will cover

1. Liability
    1. What are the fines
    2. Who is liable
2. Vendor Management (EMR providers)
3. Data logging
4. Internal Auditing
5. Protecting your logs

6. Data Retention periods

The Personal Health Information Protection Act (PHIPA) in Canada is a law that governs the collection, use, and disclosure of personal health information (PHI) by healthcare providers and other organizations involved in healthcare services. From an IT perspective, compliance with PHIPA involves several key requirements that must be tracked, implemented, and maintained.

User Access Tracking:

- Track every access to patient files by users (e.g., doctors, nurses, administrative staff).
- Record what specific patient information was accessed or viewed.
- Log time and date of access for each interaction with patient data.
- Capture any modifications made to patient files, detailing the specific changes.

Audit Capabilities:

- Enable audit trails to review who accessed a particular patient file.
- Provide details of what specific information was seen or interacted with by each user.
- Identify any changes or updates made to the patient records and when these modifications occurred.
- Ensure the ability to trace access back to individual users for accountability.

Data Integrity and Security:

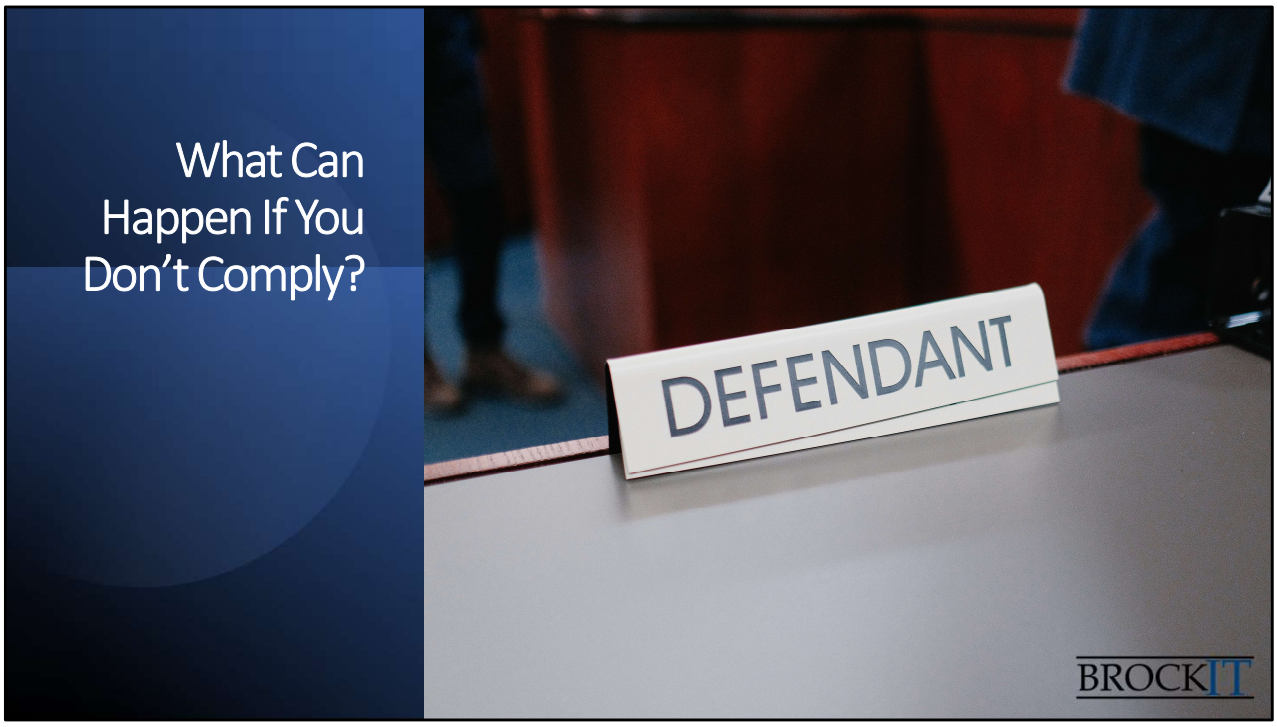
- Ensure encryption and secure storage of audit logs to prevent tampering.
- Implement user authentication measures (e.g., two-factor authentication) to verify identity before accessing sensitive data.
- Define roles and permissions clearly to limit access based on job requirements.
- Regularly review and update access permissions and audit logs for compliance.

Reporting and Breach Notification:

- Have mechanisms in place to generate reports for compliance checks.
- Establish procedures for detecting, reporting, and responding to data breaches involving patient information.
- Notify affected individuals and the relevant regulatory bodies if patient data is accessed or modified without authorization.

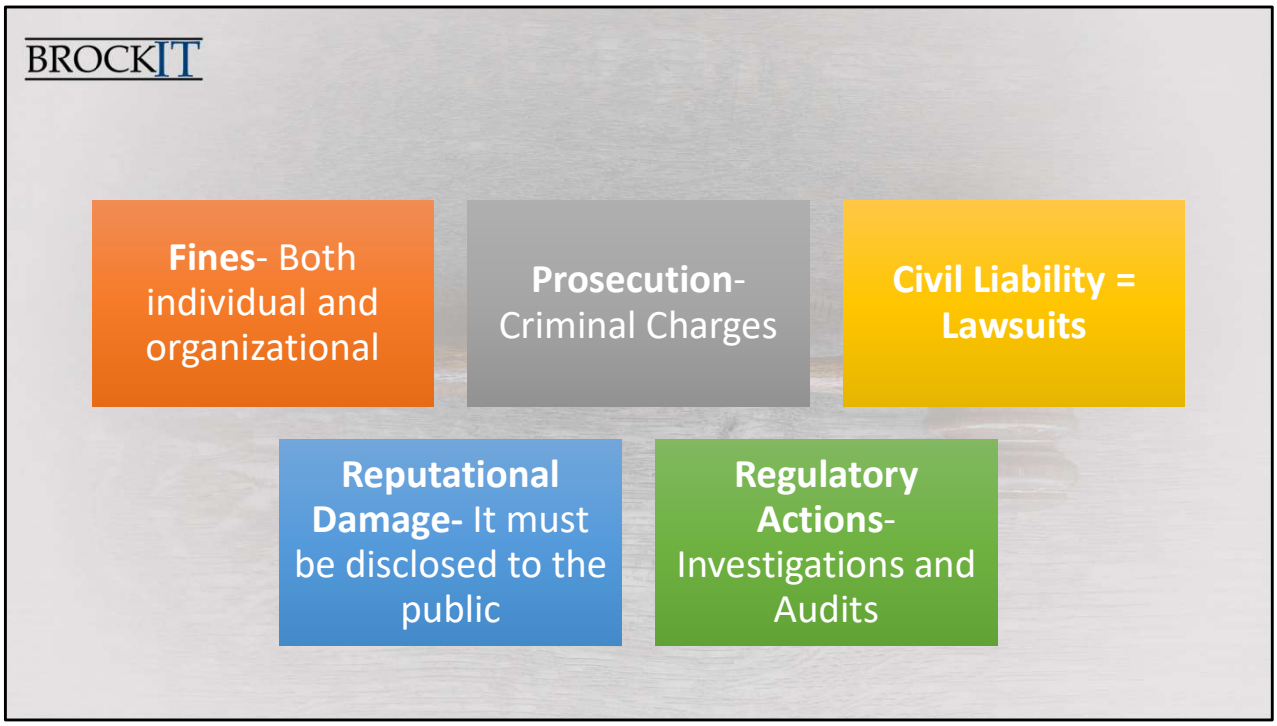
Retention and Disposal of Records:

- Maintain audit logs and access records for a minimum duration as specified by PHIPA.
- Ensure secure deletion and disposal of data records, including audit logs, when no longer required.



Punishments for Non-Compliance

PHIPA includes penalties for non-compliance, which can be imposed on both individuals and organizations. The penalties can be severe and include the following:



Punishments for Non-Compliance

PHIPA includes penalties for non-compliance, which can be imposed on both individuals and organizations. The penalties can be severe and include the following:

1. Fines

Individuals: Fines of up to CAD 100,000 for individuals found guilty of an offense under PHIPA.

Organizations: Fines of up to CAD 500,000 for organizations found guilty of an offense under PHIPA.

2. Prosecution

Criminal Charges: Individuals or organizations may face criminal charges if they

willfully breach PHIPA requirements, leading to criminal records and additional penalties.

3. Civil Liability

Lawsuits: Individuals may bring civil lawsuits against organizations for damages resulting from a breach of their privacy under PHIPA. Organizations may be liable for compensatory damages, including damages for emotional distress.

4. Reputational Damage

Public Disclosure: The Office of the Information and Privacy Commissioner of Ontario (IPC) has the authority to make public the details of breaches and the organizations involved, leading to significant reputational damage.

5. Regulatory Actions

Investigations and Audits: The IPC can conduct investigations and audits of organizations to ensure compliance with PHIPA. Non-compliant organizations may be subject to further penalties and corrective actions as mandated by the IPC.

- College of Nurses of Ontario as well.

Ensuring compliance with PHIPA requires a comprehensive approach that integrates technical, administrative, and organizational measures. Failure to comply can result in severe penalties, including substantial fines, legal actions, and reputational harm.

Who is Liable?

BROCKIT

You are. Period.

BROCKIT

Your Organization is the Custodian of Data: As a healthcare provider, your organization is considered the custodian of all patient data you collect, store, or process. This means you are legally responsible for the privacy, security, and integrity of that data.

Responsibility Beyond Software Vendors:

- Even when using third-party SaaS solutions like PCC, Epic, or other Electronic Medical Record (EMR) systems, your organization is still accountable for the security and privacy of patient information.
- These service providers may offer secure platforms, but the responsibility to ensure that patient data remains protected within those systems lies with your organization.

Liability in Case of Data Breach:

- If a data breach or unauthorized access occurs, your organization is held liable under regulations like PHIPA, regardless of the third-party tools you use.
- This includes incidents like improper access control, insufficient data encryption, or failures to monitor user access to sensitive patient data.

Importance of Vendor Management:

- While your SaaS providers must maintain their own security standards, it's crucial that your organization thoroughly assesses and manages these relationships to ensure compliance.
- Establish clear data protection agreements with service providers, but remember that these contracts do not shift liability for compliance away from your organization.

PHIPA does not directly specify technical standards or certifications that SaaS EMR providers must meet to confirm acceptable risk. However, it sets out general requirements for healthcare custodians to ensure the privacy and security of personal health information (PHI). Here's how these requirements translate into guidance for choosing SaaS EMR providers:

1.Reasonable Safeguards:

1. PHIPA requires custodians to ensure that **reasonable safeguards** are in place to protect PHI, including when using third-party services like SaaS EMR providers.
2. This means that healthcare organizations must ensure that the SaaS provider can demonstrate that they have robust measures in place to protect the confidentiality, integrity, and availability of PHI.

2.Due Diligence and Vendor Assessment:

1. Healthcare custodians are expected to conduct **due diligence** when selecting SaaS providers, which may include reviewing:
    1. **Data encryption standards** (e.g., encryption of data at rest and in transit).
    2. **Access controls** (e.g., user authentication, role-based access).
    3. **Data backup and disaster recovery** capabilities.
    4. **Physical security** of data centers if data is hosted offsite.

3.Contractual Obligations:

1. Under PHIPA, custodians must ensure that **contracts** or agreements with SaaS

EMR providers include provisions that safeguard the privacy and security of PHI.

2. The agreement should outline the provider's responsibilities, such as:
    1. Compliance with **relevant privacy and security standards**.
    2. Reporting any **breaches or security incidents** promptly.
    3. Ensuring data is **stored in jurisdictions** that comply with Canadian privacy laws.

1.Industry Standards and Certifications:

1. While PHIPA does not mandate specific certifications, it is best practice for healthcare organizations to look for SaaS EMR providers that comply with recognized industry standards, such as:
    1. **ISO 27001**: Information security management.
    2. **SOC 2**: Service Organization Control (SOC) reports focused on data security, availability, and privacy.
    3. **NIST Cybersecurity Framework**: A set of best practices for managing and reducing cybersecurity risks.
    4. **CSA STAR**: Certification from the Cloud Security Alliance, which indicates strong security practices in cloud environments.
    5. **HIPAA:** American healthy security standard with extremely detailed and robust controls.

2.PHIPA-Specific Requirements:

1. The organization should confirm that the SaaS provider understands and supports **PHIPA-specific requirements**, such as audit logging, access tracking, and secure disposal of records.
2. The SaaS solution should facilitate the custodian's ability to **track access to PHI**, allowing compliance with the audit requirements under PHIPA.

While PHIPA does not dictate specific standards for SaaS providers, it places the responsibility on healthcare organizations to verify that their chosen vendors have robust security measures that align with the legislation's requirements for protecting personal health information.

What do you need to be concerned about from an IT Perspective?

User Access Tracking

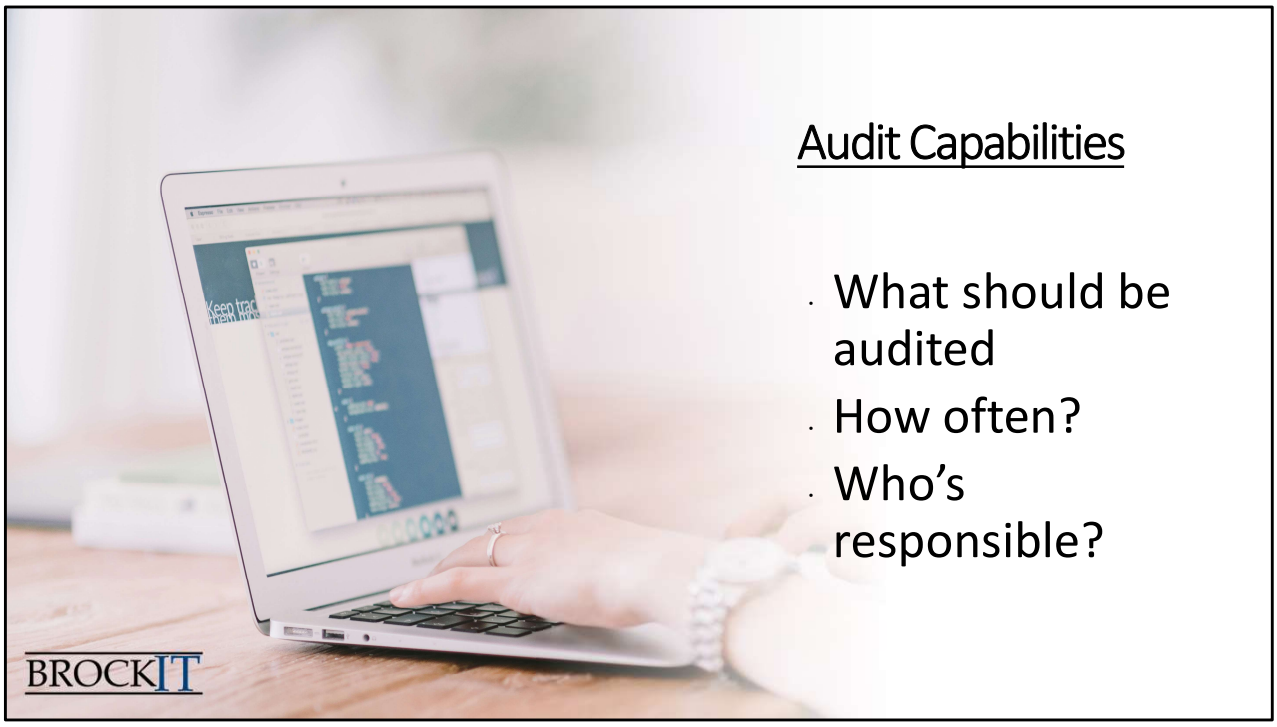
BROCKIT

- Who
- What
- Where
- When

User Access Tracking:

All access must follow the WWWW methods.

- Track every access to patient files by users (e.g., doctors, nurses, administrative staff). -> The Who
- Record what specific patient information was accessed or viewed. -> The What
- Capture any modifications made to patient files, detailing the specific changes. -> The Where
- Log time and date of access for each interaction with patient data. -> The When



Audit Capabilities

What should be audited?

- Enable audit trails to review who accessed a particular patient file.
- Provide details of what specific information was seen or interacted with by each user.
- Identify any changes or updates made to the patient records and when these modifications occurred.
- Ensure the ability to trace access back to individual users for accountability.

How often should it be audited?

PHIPA doesn't specifically mention exact timelines but legal experts have concluded that it is implied and therefore expected to be done at least annually.

- Conduct internal audits of PHIPA compliance at least **annually** to ensure that

policies and procedures are being followed.

- Some organizations opt for more frequent audits (e.g., **quarterly** or **semi-annually**) depending on the volume of patient data they manage and the complexity of their systems.

Who should be auditing?

Your privacy officer.

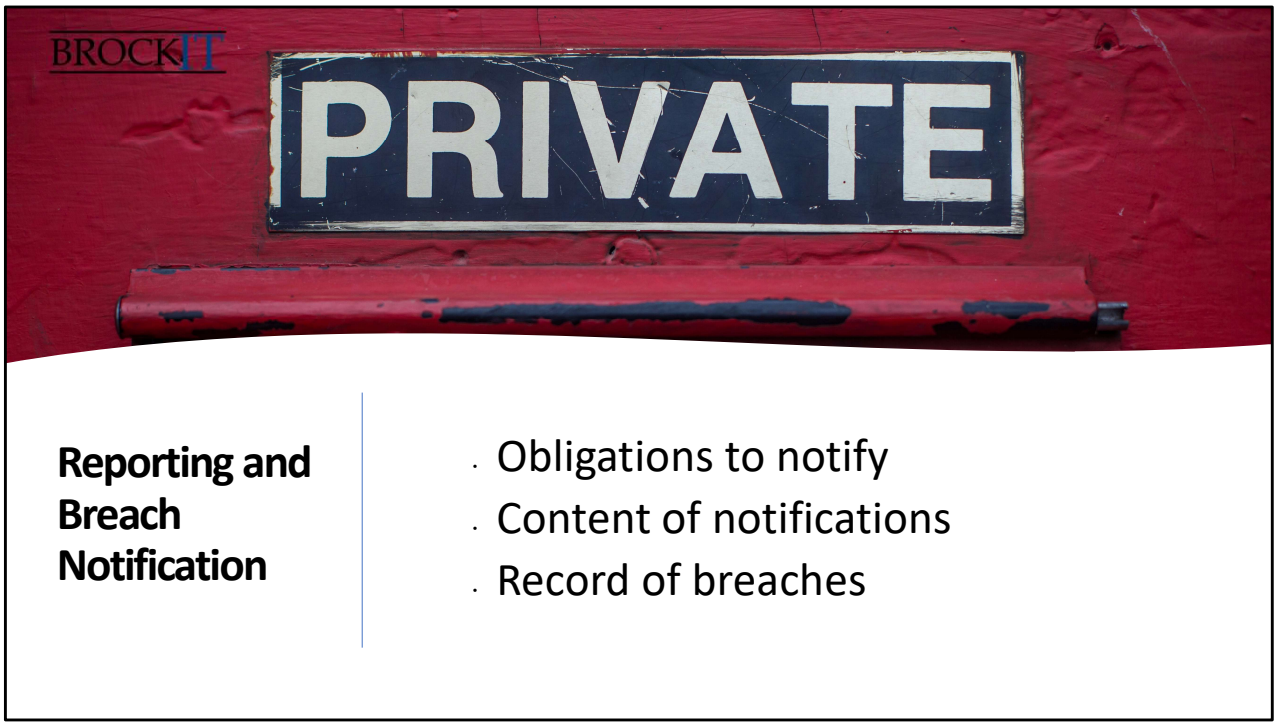
Who specifically that is depends entirely on your organization but they're **responsible** for the auditing to be done. Many orgs decide to have their QA nurse perform the audit and present the findings to the privacy officer.

Data Integrity

- Immutable logs
- Limited Access
- Review Permissions

BROCKIT

- Ensure encryption and secure storage of audit logs to prevent tampering.
- Implement user authentication measures (e.g., two-factor authentication) to verify identity before accessing sensitive data.
- Define roles and permissions clearly to limit access based on job requirements.
- Regularly review and update access permissions and audit logs for compliance.



Under PHIPA, there are specific requirements for reporting breaches involving personal health information (PHI). Here's a breakdown of the key requirements:

1. Obligation to Notify Individuals:

•**When to Notify**: Healthcare custodians must notify individuals if their personal health information has been accessed, used, disclosed, or stolen without authorization.

•**Criteria for Notification**: Notification is required if there is a **risk of harm** to the individual, which can **include risks like identity theft, financial loss, or reputational harm. THAT MEANS EVERY TIME**

•**Timeliness**: Notification to affected individuals should be made **as soon as reasonably possible** after discovering the breach.

2. Content of the Notification:

•The notification should include enough information for the individual to understand:

- **What happened** (general nature of the breach).
- **What information was affected**.
- **Steps taken** to mitigate the breach.
- **How the individual can protect themselves** (if applicable).
- **Contact information** for further assistance.

3. Notification to the Information and Privacy Commissioner of Ontario (IPC):

•**Mandatory Reporting**: As of **October 1, 2017**, PHIPA requires custodians to report certain types of breaches to the IPC. These include, but are not limited to:

- Incidents involving the **theft or loss of PHI**.
- Repeated incidents of **unauthorized access**, such as "snooping" by staff.
- **Unauthorized disclosure** of PHI due to human error or system failures.

•**Timing**: The IPC must be notified **as soon as reasonably possible** after the breach is detected.

4. Notification to Professional Regulatory Colleges:

•If a breach involves a regulated health professional (e.g., a doctor, nurse) and it meets specific criteria of intentional or repeated unauthorized access, the healthcare custodian must notify the relevant **professional regulatory college**.

5. Record-Keeping Requirements:

•Custodians must **keep a record of all breaches**, even if they are not reportable to the IPC or do not meet the threshold for notifying affected individuals.

•These records must be kept for at least **two years** and made available to the IPC upon request.

Summary of Who Needs to Be Informed:

•**Affected Individuals**: When there is a risk of harm due to the breach.

•**Information and Privacy Commissioner of Ontario (IPC)**: For specific breaches as mandated (e.g., theft, snooping).

•**Professional Regulatory College**: When the breach involves a regulated health professional under specific conditions.

These measures ensure that individuals are informed of risks to their personal information, that oversight bodies are aware of significant breaches, and that healthcare organizations are accountable for maintaining the security and privacy of personal health information.

Under the **College of Nurses of Ontario (CNO)**, there are specific requirements and obligations for nurses related to the handling of personal health information (PHI), particularly when it comes to **privacy breaches** under PHIPA. Here's an overview of key responsibilities and considerations for nurses in Ontario:

1. Duty to Report Breaches:

•Nurses have an **ethical and professional obligation** to protect patient privacy and confidentiality, as outlined by the CNO's **Practice Standard: Confidentiality and Privacy – Personal Health Information**.

•If a nurse becomes aware of a **breach of patient privacy**, they have a duty to report the breach within their organization according to its internal policies and procedures.

•Nurses must also **cooperate with investigations** into breaches of privacy conducted by their employer or by regulatory authorities like the Information and Privacy Commissioner of Ontario (IPC).

2. Mandatory Notification to CNO:

•Under PHIPA, there are situations where **health information custodians** (e.g., hospitals, clinics) are required to notify a professional **regulatory college**, such as the CNO, if a privacy breach involves a **regulated health professional**.

•**When is this Required?**:

- If a nurse engages in **intentional or willful unauthorized access** to a patient's health information, commonly known as "snooping."
- If a nurse is involved in **multiple or repeated breaches** of privacy.

•The custodian must inform the CNO **as soon as reasonably possible** after determining that the breach meets these criteria.

3. Professional Misconduct and Disciplinary Actions:

•The CNO treats privacy breaches, especially intentional unauthorized access, as **professional misconduct**.

•**Possible Consequences** include:

- Disciplinary action by the CNO, which may include **reprimands, suspensions, or revocation of the nurse's registration**.
- **Formal hearings** for serious breaches, where the nurse may have to respond to allegations of misconduct.
- Mandatory **reporting to the CNO** can result in additional scrutiny on the nurse's practice and possibly impact their professional standing.

4. Responsibilities for Nurses in Supervisory Roles:

•Nurses in supervisory or leadership positions (e.g., nurse managers) have an added responsibility to ensure that their teams are trained on PHIPA compliance and understand the **importance of safeguarding patient information**.

•They must also ensure that appropriate **policies and procedures** are in place for reporting breaches and that these policies are effectively communicated to their teams.

Summary of CNO-Related Requirements:

•Nurses must **report breaches internally** and cooperate with organizational and regulatory investigations.

•**Health information custodians** must notify the CNO if a nurse engages in intentional or repeated privacy breaches.

•The CNO may take disciplinary actions against nurses involved in unauthorized access or mishandling of PHI, treating such incidents as professional misconduct.

Maintain audit logs and access records for a minimum duration as specified by PHIPA.

PHIPA does not specify an exact duration for retaining audit logs. However, the general best practice, aligned with other data privacy standards and guidelines, suggests the following:

1.Recommended Retention Period:

1. Maintain audit logs for a minimum of **7 to 10 years**. This duration aligns with the retention periods often recommended for medical records and is considered a standard in healthcare settings.

2.Longer Retention for Specific Cases:

1. If audit logs are involved in legal proceedings, investigations, or a privacy complaint, they should be retained **until the matter is resolved** and for an additional period if required by legal counsel.

3.Alignment with Organizational Policy:

1. The specific retention period should be documented in your organization's data retention policy and aligned with other records management practices.
2. It's also crucial to ensure that audit logs remain accessible and are stored securely during their retention period to comply with data protection

obligations.

By maintaining audit logs for a sufficient duration, organizations can demonstrate compliance with PHIPA and ensure accountability for access and modifications to personal health information.

Ensure secure deletion and disposal of data records, including audit logs, when no longer required.

PHIPA does not provide specific technical details or methods for secure deletion and disposal of data records and audit logs. However, it does mandate that healthcare custodians take **reasonable steps to protect personal health information** (PHI), which includes secure disposal. The key principles include:

1.Reasonable Security Measures:

1. Organizations must take **reasonable steps** to ensure that PHI is protected against theft, loss, and unauthorized access during the **disposal** process. This implies using secure methods for data destruction.

2.Secure Disposal Methods:

1. While PHIPA does not specify exact methods, best practices for secure disposal generally include:
    1. **Data Wiping**: Using software tools to overwrite data on digital storage devices (e.g., hard drives, SSDs) multiple times to prevent recovery.
    2. **Physical Destruction**: Shredding, pulverizing, or incinerating storage media like hard drives, CDs, or printed records to render them unreadable.
    3. **Decommissioning**: Ensuring that decommissioned systems, such as old servers or storage devices, undergo secure data erasure before they are discarded or repurposed.

3.Policy Development:

1. Healthcare organizations are expected to **develop and implement policies and procedures** that outline how data records and audit logs should be securely deleted or disposed of.

2. These policies should include a description of the secure deletion methods used, the responsibilities of staff, and any verification processes to ensure proper disposal.

1.Third-Party Disposal:

1. If using third-party services for data destruction, PHIPA requires that the custodian ensure that these services provide **adequate guarantees** that the data will be securely destroyed, often formalized through agreements or certifications.

Though PHIPA leaves the specifics up to the organization, adherence to these principles and aligning with industry best practices ensures compliance and minimizes the risk of data breaches during the disposal process.

Questions?

Like some more information?

Reach out to:
William Thomson
William@brock-it.ca
613-499-9960 x115

Sign up for the Next Webinar:

Managing PHIPA Breaches: Essential Steps

Like & Follow Us on Social Media

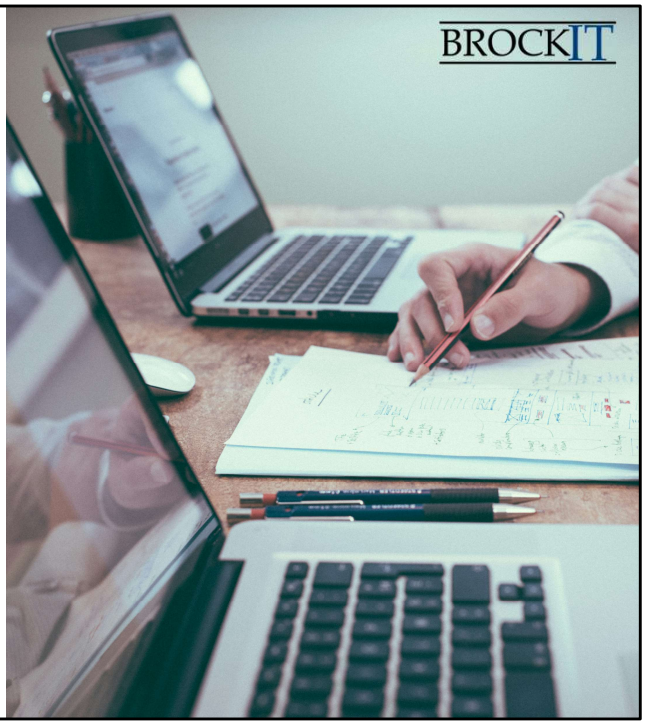
Facebook
LinkedIn

BROCKIT

Training and Awareness

Staff Training

Awareness Programs



Training and Awareness

- **Staff Training:** Regularly train staff on PHIPA requirements and best practices for handling PHI. Ensure that all personnel understand their responsibilities under the law.
- **Awareness Programs:** Implement ongoing awareness programs to keep staff informed about data protection and privacy issues.

Incident Management

Incident Response Plan

Continuous Monitoring

BROCKIT

Incident Management

- **Incident Response Plan:** Develop and maintain an incident response plan that outlines procedures for responding to data breaches and other security incidents involving PHI.
- **Continuous Monitoring:** Implement continuous monitoring of IT systems to detect and respond to unauthorized access or other security threats.